

PCT/NL

03/00447

KONINKRIJK DER



NEDERLANDEN

Bureau voor de Industriële Eigendom



REC'D 30 JUL 2003

WIPO PCT

Hierbij wordt verklaard, dat in Nederland op 19 juni 2002 onder nummer 1020903,

ten name van:

ENSCHEDÉ/SDU B.V.

te Haarlem

een aanvraag om octrooi werd ingediend voor:

"Systeem en werkwijze voor het automatisch verifiëren van de houder van een autorisatiedocument en het automatisch vaststellen van de authenticiteit en geldigheid van het autorisatiedocument",

en dat de hieraan gehechte stukken overeenstemmen met de oorspronkelijk ingediende stukken.

BEST AVAILABLE COPY

Rijswijk, 10 juli 2003

De Directeur van het Bureau voor de Industriële Eigendom,
voor deze,

Mw. I.W. Scheevelenbos-de Reus

**PRIORITY
DOCUMENT**

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

1020903

B. v.d. I.E.

19 JUNI 2002

Uittreksel

- Systeem voor het uitlezen van een document voorzien van machine-leesbare houdergegevens en het vaststellen of een aanbieder van het document een vooraf
- 5 bepaald recht heeft, welk document tenminste een chip met biometrische gegevens van een houder alsmede data met een vooraf bepaalde relatie tot de houdergegevens omvat en waarbij het systeem omvat:
- een uitleeseenheid voor het uitlezen van de chip en van de machine-leesbare houdergegevens;
 - 10 • een geheugen met gegevens omtrent het recht van de houder;
 - een biometrische kenmerk scanner;
 - een verwerkingseenheid, verbonden met uitleeseenheid, geheugen en scanner en ingericht om:
 - 15 • met publieke sleutel coderingstechnologie de authenticiteit van chip en data vast te stellen;
 - de biometrische gegevens van de houder uit de chip te ontvangen;
 - de biometrische gegevens van de aanbieder van het document te ontvangen van de scanner en te vergelijken met de gegevens van de houder om te bepalen of de aanbieder de houder is;
 - 20 • het ontvangen van de houdergegevens via de uitleeseenheid, het controleren van de relatie tussen de houdergegevens en de data en het lezen van het recht van de houder uit het geheugen;
- het verschaffen van een signaal ter indicatie van het recht voor de aanbieder, als de chip en de data authentiek zijn, de relatie is vastgesteld en de aanbieder gelijk is aan de hou-
- 25 der.

Systeem en werkwijze voor het automatisch verifiëren van de houder van een autorisatiedocument en het automatisch vaststellen van de authenticiteit en geldigheid van het autorisatiedocument

5 **Stand van de techniek**

Het systeem en de werkwijze waarop de uitvinding betrekking heeft vindt vooral toepassing bij het controleren van paspoorten bij een grenspassage. De uitvinding kan echter ook worden toegepast bij het verkrijgen van toegang tot een bepaalde locatie of ruimte, of het verkrijgen van een recht van toegang tot een systeem, zoals een computer of een terminal, etc.

De methode die algemeen wordt gevolgd door een controleur bij grenspassage is als volgt:

- 15 A. Controle op de authenticiteit van een reisdocument en controle op de authenticiteit van de informatie opgenomen in een reisdocument, zoals een paspoort, door het bekijken van echtheidskenmerken;
- B. Verificatie of het document dat wordt aangeboden wel hoort bij degene die het aanbiedt (houder), door vergelijking van de pasfoto en/of handtekening;
- 20 C. Controle van de geldigheid van het document en de toestemming voor grenspassage door het paspoortnummer en/of de naam van de houder te toetsen tegen een database met negatief register, d.w.z. een register waarin een lijst met paspoortnummers en/of persoonsnamen is opgenomen van houders die niet tot de grensovergang geautoriseerd zijn.

25

Toepassing van biometrie op een paspoort, in aanvulling op een pasfoto en handtekening, is eveneens bekend en dient ter ondersteuning voor stap B, het verifiëren van de documenthouder. Bekende biometrische werkwijzen, die ook bij de uitvinding kunnen worden gebruikt, omvatten bijvoorbeeld het gebruik van een of meer van de volgende persoonskenmerken (biometrische template): ogen (iris), spraak, handafdrukken, vingerafdrukken, gelaat en hand-geschreven handtekeningen.

30

Een voor de hand liggende uitvoering van een reisdocument met biometrie is het op-

slaan van de biometrische template op het document. Dit kan bijvoorbeeld in een 2D-barcode, op een magneetstrip of in een chip.

5 Bij automatische controle is een nadeel hiervan dat de biometrische template gekoppeld is met de persoonsgegevens. Dit kan ongewenst zijn in verband met de privacy. Een ander nadeel is dat een biometrisch template van een onbevoegde aan een reisdocument kan worden toegevoegd, zodat deze onbevoegde onterecht een grens kan passeren. Ook kan elk willekeurig ander (fake) document met biometrische template worden aangeboden. Deze vormen van fraude blijven dan bij automatische controle onopgemerkt.

10

Korte samenvatting van de uitvinding.

De uitvinding heeft daarom tot doel om een systeem te verschaffen dat de voornoemde nadelen niet heeft.

15

Daartoe verschaft de uitvinding allereerst een systeem voor het uitlezen van een document voorzien van machine-leesbare houdergegevens en het vaststellen of een aanbieder van het document een vooraf bepaald recht heeft, welk document tenminste een chip met biometrische gegevens van een houder alsmede data met een vooraf

20 bepaalde relatie tot de houdergegevens omvat, en waarbij het systeem omvat:

- een uitleeseenheid voor het uitlezen van de chip en van de machine-leesbare houdergegevens;
- een geheugen met gegevens omtrent het vooraf bepaalde recht van de houder;
- een biometrische kenmerk scanner;
- 25 • een verwerkingseenheid, die met de uitleeseenheid, het geheugen en de biometrische kenmerk scanner is verbonden en is ingericht om:
 - met behulp van een publieke sleutel coderingstechnologie de authenticiteit van de chip en de data vast te stellen;
 - de biometrische gegevens van de houder uit de chip te ontvangen van de uitleeseenheid;
 - 30 • de biometrische gegevens van de aanbieder van het document te ontvangen van de biometrische kenmerk scanner en te vergelijken met de biometrische gegevens van de houder om te bepalen of de aanbieder de houder is;

- het ontvangen van de houdergegevens via de uitleeseenheid, het controleren van de vooraf bepaalde relatie tussen de houdergegevens en de data en het lezen van het vooraf bepaalde recht van de houder uit het geheugen;
- het verschaffen van een signaal ter indicatie van het vooraf bepaalde recht voor de aanbieder, als de chip en de data authentiek zijn, de vooraf bepaalde relatie is vastgesteld en de aanbieder gelijk is aan de houder.

In een uitvoeringsvorm heeft de uitvinding betrekking op een werkwijze voor het uitlezen van een document voorzien van machine-leesbare houdergegevens en het vaststellen of een aanbieder van het document een vooraf bepaald recht heeft, welk document tenminste een chip met biometrische gegevens van een houder alsmede data met een vooraf bepaalde relatie tot de houdergegevens omvat, en waarbij het systeem omvat een uitleeseenheid voor het uitlezen van de chip en van de machine-leesbare houdergegevens, een geheugen met gegevens omtrent het vooraf bepaalde recht van de houder, een biometrische kenmerk scanner, en een verwerkingseenheid, die met de uitleeseenheid, het geheugen en de biometrische kenmerk scanner is verbonden, waarbij de werkwijze de volgende handelingen omvat:

- vaststellen van de authenticiteit van de chip en de data met behulp van een publieke sleutel coderingstechnologie;
- ontvangen van de biometrische gegevens van de houder uit de chip;
- ontvangen van de biometrische gegevens van de aanbieder van het document en het vergelijken met de biometrische gegevens van de houder om te bepalen of de aanbieder de houder is;
- het ontvangen van de houdergegevens, het controleren van de bepaalde relatie tussen de houdergegevens en de data en het lezen van het vooraf bepaalde recht van de houder uit het geheugen;
- het verschaffen van een signaal ter indicatie van het vooraf bepaalde recht voor de aanbieder, als de chip en de data authentiek zijn, de vooraf bepaalde relatie is vastgesteld en de aanbieder gelijk is aan de houder.

In een verdere uitvoeringsvorm heeft de uitvinding betrekking op een computerprogramma dat kan worden geladen door een systeem voor het uitlezen van een document voorzien van machine-leesbare houdergegevens en het vaststellen of een

aanbieder van het document een vooraf bepaald recht heeft, welk document tenminste een chip met biometrische gegevens van een houder alsmede data met een vooraf bepaalde relatie tot de houdergegevens omvat, en waarbij het systeem omvat een uitleeseenheid voor het uitlezen van de chip en van de machine-leesbare
 5 houdergegevens, een geheugen met gegevens omtrent het vooraf bepaalde recht van de houder, een biometrische kenmerk scanner, en een verwerkingseenheid, die met de uitleeseenheid, het geheugen en de biometrische kenmerk scanner is verbonden, waarbij het computerprogramma het systeem de volgende functionaliteit kan verschaffen:

- 10 • vaststellen van de authenticiteit van de chip en de data met behulp van een publieke sleutel coderingstechnologie;
- ontvangen van de biometrische gegevens van de houder uit de chip;
- ontvangen van de biometrische gegevens van de aanbieder van het document en het vergelijken met de biometrische gegevens van de houder om te bepalen of
 15 de aanbieder de houder is;
- het ontvangen van de houdergegevens van de chip, het controleren van de bepaalde relatie tussen de houdergegevens en de data en het lezen van het vooraf bepaalde recht van de houder uit het geheugen;
- het verschaffen van een signaal ter indicatie van het vooraf bepaalde recht voor
 20 de aanbieder, als de chip en de data authentiek zijn, de vooraf bepaalde relatie is vastgesteld en de aanbieder gelijk is aan de houder.

In een nog verdere uitvoeringsvorm heeft de uitvinding betrekking op een houder voorzien van een dergelijk computerprogramma.

25

Tenslotte betreft de uitvinding ook een document voorzien van machine-leesbare houdergegevens en een chip, welke chip is voorzien van een verwerkingseenheid en daarmee verbonden geheugen en een invoer/uitvoer-eenheid, waarbij het geheugen biometrische gegevens van een houder omvat, alsmede data die een vooraf bepaalde
 30 relatie tot de houdergegevens hebben, alsmede instructies om de verwerkingseenheid de volgende handelingen te laten verrichten:

- communiceren met een systeem volgens conclusie 1 om de authenticiteit van de chip met behulp van een publieke sleutel coderingstechnologie te laten vast-

stellen;

- versturen van de biometrische gegevens van de houder en de data uit het geheugen naar het systeem.

- 5 Door de uitvinding kan automatisch worden vastgesteld dat het document authentiek is en dat de aanbieder van het document werkelijk de houder daarvan is.

Figuurbeschrijving

- 10 De uitvinding zal kort worden beschreven aan de hand van enkele figuren die slechts zijn bedoeld ter illustratie daarvan en niet ter beperking van de reikwijdte daarvan, die slechts wordt beperkt door de bijgevoegde conclusies en hun equivalenten.

15 Figuur 1 toont een document, in de vorm van een boekje, bijvoorbeeld een paspoort, waarin zich een chip met biometrische gegevens bevindt;

 Figuur 2 toont een systeem, waarmee het document, zoals getoond in figuur 1, kan worden uitgelezen en geëvalueerd;

 Figuur 3 toont een schematische voorstelling van een chip, zoals die in het document volgens figuur 1 kan worden opgenomen.

20

Beschrijving van uitvoeringsvormen

- De uitvinding zal nu worden beschreven met verwijzing naar het gebruik van een paspoort als reisdocument. Zoals eerder gezegd, kan de uitvinding echter ook breder worden toegepast, namelijk daar waar iemand een bepaald recht moet krijgen om iets te mogen doen.
- 25

Figuur 1 toont de toepassing van de uitvinding bij een paspoort 6.

- 30 Het paspoort 6, zoals getoond in figuur 1, is met uitzondering van chip 5 uitvoerig beschreven in de Europese octrooiaanvraag EP-A-1.008.459. Het paspoort zoals daar omschreven, inclusief al zijn uitvoeringsvormen, kan bij de onderhavige uitvinding worden gebruikt. Het paspoort 6 omvat een kaart 1 voorzien van tekst, een paspoortfoto en een handtekening. De kaart 1 kan bijvoorbeeld gemaakt zijn van synthetisch

laminaat. De kaart 1 is bevestigd aan een band 2, die ervoor zorgt dat de kaart in de vorm van een boekje kan worden vastgehouden. Op de kaart 1 zijn machine-leesbare houdergegevens vermeld.

5 Het boekje bevat verdere pagina's 4, geschikt om bijvoorbeeld visa voor het bezoek aan landen in op te nemen. Het boekje bevat ook een kapt 3. Voor verdere details en uitvoeringsvormen wordt de lezer verwezen naar de Europese octrooiaanvraag EP-A-1.008.459.

Opgemerkt wordt nog, dat de uitvinding ook bij andere soorten documenten kan worden toegepast, maar dat toepassing bij een paspoort (of ander reisdocument) bijzonder
10 voordelig is, omdat daarvoor tot nu toe geen waterdichte controle van de authenticiteit van het document, alsmede verificatie van de aanbieder is gevonden.

In overeenstemming met de uitvinding omvat de kaart 1 een chip 5. De chip 5 is bij voorkeur integraal in de kaart 1 opgenomen, op zodanige wijze dat deze chip 5 niet zonder beschadiging van de kaart 1 kan worden verwijderd.

15 Figuur 3 toont een uitvoeringsvorm van een dergelijke chip 5. De chip 5 omvat een verwerkingseenheid (CPU) 14, die is verbonden met een geheugen 16, alsmede met invoer/uitvoer-eenheid 15.

Het geheugen omvat bijvoorbeeld ROM en een niet-vluchtig geheugen, zoals een EEPROM, maar ook andere geheugentypes kunnen worden toegepast. In het geheugen
20 is tenminste opgeslagen: een private sleutel (bij voorkeur in ROM, zodat deze niet kan worden veranderd), een biocertificaat en (optioneel) een certificaat van een uitgevende instantie. Het biocertificaat omvat biometrische kenmerkgegevens van de houder van het paspoort en data die een vooraf bepaalde relatie met de machine-leesbare gegevens hebben.

25 De invoer/uitvoer-eenheid 15 is bij voorkeur geschikt voor contactloze communicatie met het systeem dat in figuur 2 is getoond. De invoer/uitvoer-eenheid 15 kan daartoe bij voorkeur worden gemaakt als een cirkelvormige antenne, zoals in figuur 3 is getoond. Andere uitvoeringsvormen zijn echter mogelijk. Ook contactvlakjes, zoals bekend van hedendaagse chipkaarten, zijn mogelijk.

30 Het mag duidelijk zijn, dat figuur 3 slechts een uitvoeringsvorm toont. Indien gewenst kunnen er meerdere verwerkingseenheden zijn voorzien, alsmede meerdere vormen van geheugens en meerdere invoer/uitvoer-eenheden. Bij voorkeur ontvangt de chip 5 zijn voedingsenergie van het systeem dat in figuur 2 is getoond tijdens communicatie daar-

mee. Daartoe is de chip 5 dan uitgevoerd als een transponder-eenheid. Een dergelijke transponder-eenheid is aan de deskundige bekend en hoeft hier niet uitgebreid te worden toegelicht. Uiteraard kan in plaats daarvan een batterij zijn voorzien, hoewel dit in de meeste gevallen erg onpraktisch is.

5

Figuur 2 toont een systeem 7 voor het uitlezen van de op het paspoort 6 aangebrachte chip 5.

Daartoe is het systeem volgens figuur 2 uitgerust met een kaartleeseenheid 8, die voorzien is van een chipleeseenheid om met de chip 5 van de kaart 1 te communiceren,
10 en een leeseenheid voor het lezen van de houdergegevens die bijvoorbeeld zijn vermeld in een "Machine Readable Zone" (MRZ) van de kaart 1.

De kaartleeseenheid 8 is verbonden met een verwerkingseenheid (CPU) 9. De CPU 9 is verbonden met een geheugen 10.

Het systeem 7 is tevens verbonden met een biometrisch kenmerkscanner 11, alsmede
15 een toetsenbord 12 en een scherm 13.

De biometrische kenmerkscanner 11 is ingericht om een biometrisch kenmerk van een aanbieder van het document 6 te kunnen scannen. Een dergelijke scanner 11 kan bijvoorbeeld een irisscanner zijn of een apparaat voor het uitlezen van een vingerafdruk van de aanbieder. Dergelijke biometrische kenmerkscanners 11 zijn bekend in de tech-
20 niek en behoeven hier niet in detail te worden beschreven.

De structuur van het systeem 7 uit figuur 2 is willekeurig. Indien gewenst, kunnen alle onderdelen in één kast zijn opgenomen. Sommige onderdelen kunnen ook echter naar wens in losse kasten zijn aangebracht. Behalve het toetsenbord 12 kan bijvoorbeeld ook voorzien zijn in een muis of andere invoer/uitvoer-middelen, die bij de deskundige be-
25 kend zijn. Het scherm 13 kan elke gewenste vorm hebben en van elk gewenst type zijn, dat op dit moment (of in de toekomst) op de markt te verkrijgen is.

In figuur 2 is aangegeven dat er een geheugen 10 is. Dit geheugen kan bestaan uit RAM, ROM, EEPROM, een harde schijf, etc., etc. De verwerkingseenheid 9, kan bestaan uit één enkele eenheid, maar ook uit meerdere eenheden, die al dan niet parallel
30 of in master-slave verhouding zijn opgesteld. Als verder alternatief, kunnen verschillende onderdelen op afstand van elkaar zijn aangebracht. Het geheugen 10 kan bijvoorbeeld op grote afstand zijn gelokaliseerd, indien dat gewenst is.

Nu zal de werking van het systeem volgens figuur 2 aan de hand van een aantal handelingen worden toegelicht.

- 5 1. Het paspoort 6 wordt aangeboden aan de kaartleeseenheid 8 voor het lezen van de houdergegevens uit de MRZ en het lezen van gegevens uit de chip 5 op het paspoort 6;
2. De uitgelezen gegevens worden naar de CPU 9 gestuurd;
3. De CPU 9 stuurt via de chipleeseenheid een random challenge code naar de chip 5 ter controle van de authenticiteit van chip 5 en vraagt de chip 5 om deze
10 met de op de chip 5 opgeslagen private sleutel behorend bij het aldaar opgeslagen biocertificaat digitaal te ondertekenen of te vercijferen;
4. Daarna stuurt de chip 5 de met de private sleutel vercijferde of digitaal ondertekende challenge code terug naar de CPU 9. De vercijferde of digitaal ondertekende challenge code is de digitale response. De chip 5 stuurt eveneens
15 het met de private sleutel van de uitgevende instantie ondertekende biocertificaat zoals opgeslagen op de chip naar de CPU 9. Optioneel wordt ook het certificaat van de uitgevende instantie van het paspoort door de chip 5 naar de CPU 9 gestuurd. De volgorde waarin deze gegevens door de chip 5 naar de CPU 9 worden gestuurd is willekeurig. Ook hoeft niet persé van één private
20 sleutel gebruik te worden gemaakt;
5. De CPU 9 controleert met behulp het certificaat van de uitgevende instantie of het biocertificaat en de data die daarin is opgeslagen authentiek zijn;
6. De CPU 9 controleert met behulp van het biocertificaat of de digitale response correct is;
- 25 7. In het biocertificaat zijn data opgeslagen aan de hand waarvan de relatie tussen het biocertificaat en de houdergegevens te controleren is. Dit kan bijvoorbeeld in de vorm van een HASH over de houdergegevens. De CPU 9 controleert met behulp van de data in het biocertificaat en de houdergegevens de relatie tussen het biocertificaat en de houdergegevens. Hiermee wordt tevens de authenticiteit
30 van de houdergegevens vastgesteld.
8. Het biometrische kenmerk van de aanbieder van het paspoort wordt gelezen met de biometrische kenmerk scanner 11 en deze stuurt de gegevens naar de CPU 9. De CPU 9 zet deze om in een biometrisch template (uiteeraard kan de

functionaliteit voor het omzetten daarvan ook in de biometrische kenmerk scanner 11 worden opgenomen, door deze van geschikte intelligentie daarvoor te voorzien);

- 5 9. De CPU 9 controleert, bij voorkeur via een één-wegsfunctie (bijvoorbeeld een HASH-functie) of het paspoortnummer en/of de houder in het in geheugen 10 opgeslagen negatieve register voorkomt en meldt dit aan de controleur, bijvoorbeeld via scherm 13;
- 10 10. De CPU 9 controleert of het uit handeling 8 verkregen biometrische template overeenkomt met het biometrische template uit het van de chip 5 ontvangen biocertificaat; de uitslag van deze controle wordt meegedeeld aan de controleur, bij voorkeur via scherm 13.

De uitvinding heft de nadelen op die zich bij de "stand van de techniek" voordoen. Door de bovengenoemde handelingen kan namelijk gecontroleerd worden dat én het
15 paspoort én de houdergegevens authentiek zijn en de aanbieder van het paspoort ook werkelijk de houder daarvan is. Dat wil zeggen dat veilige automatische grenscontrole hiermee mogelijk wordt, hetgeen tot op heden (nog) niet het geval was.

Door toepassing van het "biocertificaat", is de biometrische template niet direct
20 gekoppeld met de persoonsgegevens. Dit is mede het geval doordat de relatie tussen het biocertificaat en de houdergegevens (bijvoorbeeld de data in de MRZ) met een één-wegsfunctie (HASH) aan elkaar gekoppeld zijn.

Door ondertekening van de challenge code met de private sleutel wordt de authenticiteit van de informatiedrager (chip) gecontroleerd. De private sleutel is niet kopieerbaar.
25 Door de controle van biocertificaat met biometrisch template en de controle van de authenticiteit van de chip 5 is fraude bij automatische controle nagenoeg uitgesloten. Bovendien zijn chip 5 en het paspoort 6 onlosmakelijk met elkaar verbonden, waardoor manipulatie van de chip 5 onmogelijk wordt zonder herkenbare schade aan te richten.

Conclusies

1. Systeem voor het uitlezen van een document (6) voorzien van machine-leesbare houdergegevens en het vaststellen of een aanbieder van het document (6) een vooraf
 5 bepaald recht heeft, welk document tenminste een chip (5) met biometrische gegevens van een houder alsmede data met een vooraf bepaalde relatie tot de houdergegevens omvat en waarbij het systeem omvat:
 - een uitleeseenheid (8) voor het uitlezen van de chip (5) en van de machine-leesbare houdergegevens;
 - 10 • een geheugen (10) met gegevens omtrent het vooraf bepaalde recht van de houder;
 - een biometrische kenmerk scanner (11);
 - een verwerkingseenheid (9), die met de uitleeseenheid (8), het geheugen (10) en de biometrische kenmerk scanner (11) is verbonden en is ingericht om:
 - met behulp van een publieke sleutel coderingstechnologie de authenticiteit van
 15 de chip en de data vast te stellen;
 - de biometrische gegevens van de houder uit de chip te ontvangen van de uitleeseenheid (8);
 - de biometrische gegevens van de aanbieder van het document te ontvangen van de biometrische kenmerk scanner (11) en te vergelijken met de biometrische
 20 gegevens van de houder om te bepalen of de aanbieder de houder is;
 - het ontvangen van de houdergegevens via de uitleeseenheid (8), het controleren van de vooraf bepaalde relatie tussen de houdergegevens en de data en het lezen van het vooraf bepaalde recht van de houder uit het geheugen (10);
 - het verschaffen van een signaal ter indicatie van het vooraf bepaalde recht voor
 25 de aanbieder, als de chip (5) en de data authentiek zijn, de vooraf bepaalde relatie is vastgesteld en de aanbieder gelijk is aan de houder.
2. Systeem volgens conclusie 1, waarbij het document een reisdocument is.
- 30 3. Systeem volgens conclusie 1 of 2, waarbij de verwerkingseenheid (9) is ingericht om de houdergegevens met een één-wegsfunctie te vergelijken met in het geheugen (10) opgeslagen houdergegevens.

4. Systeem volgens conclusie 3, waarbij de één-wegsfunctie een HASH-functie is.

5. Werkwijze voor het uitlezen van een document (6) voorzien van machine-leesbare houdergegevens en het vaststellen of een aanbieder van het document (6) een
5 vooraf bepaald recht heeft, welk document tenminste een chip (5) met biometrische gegevens van een houder alsmede data met een vooraf bepaalde relatie tot de houdergegevens omvat, en waarbij het systeem omvat een uitleeseenheid (8) voor het uitlezen van de chip (5) en van de machine-leesbare houdergegevens, een geheugen (10) met gegevens omtrent het vooraf bepaalde recht van de houder, een biometrische
10 kenmerk scanner (11), en een verwerkingseenheid (9), die met de uitleeseenheid (8), het geheugen (10) en de biometrische kenmerk scanner (11) is verbonden, waarbij de werkwijze de volgende handelingen omvat:

- vaststellen van de authenticiteit van de chip en de data met behulp van een publieke sleutel coderingstechnologie;
- 15 • ontvangen van de biometrische gegevens van de houder uit de chip;
- ontvangen van de biometrische gegevens van de aanbieder van het document en het vergelijken met de biometrische gegevens van de houder om te bepalen of de aanbieder de houder is;
- het ontvangen van de houdergegevens, het controleren van de bepaalde relatie
20 tussen de houdergegevens en de data en het lezen van het vooraf bepaalde recht van de houder uit het geheugen (10);
- het verschaffen van een signaal ter indicatie van het vooraf bepaalde recht voor de aanbieder, als de chip (5) en de data authentiek zijn, de vooraf bepaalde relatie is vastgesteld en de aanbieder gelijk is aan de houder.

25

6. Computerprogramma dat kan worden geladen door een systeem voor het uitlezen van een document (6) voorzien van machine-leesbare houdergegevens en het vaststellen of een aanbieder van het document (6) een vooraf bepaald recht heeft, welk document tenminste een chip (5) met biometrische gegevens van een houder alsmede
30 data met een vooraf bepaalde relatie tot de houdergegevens omvat, en waarbij het systeem omvat een uitleeseenheid (8) voor het uitlezen van de chip (5) en van de machine-leesbare houdergegevens, een geheugen (10) met gegevens omtrent het vooraf bepaalde recht van de houder, een biometrische kenmerk scanner (11), en een

verwerkingseenheid (9), die met de uitleeseenheid (8), het geheugen (10) en de biometrische kenmerk scanner (11) is verbonden, waarbij het computerprogramma het systeem de volgende functionaliteit kan verschaffen:

- 5 • vaststellen van de authenticiteit van de chip (5) en de data met behulp van een publieke sleutel coderingstechnologie;
- ontvangen van de biometrische gegevens van de houder uit de chip;
- ontvangen van de biometrische gegevens van de aanbieder van het document en het vergelijken met de biometrische gegevens van de houder om te bepalen of de aanbieder de houder is;
- 10 • het ontvangen van de houdergegevens van de chip (5), het controleren van de bepaalde relatie tussen de houdergegevens en de data en het lezen van het vooraf bepaalde recht van de houder uit het geheugen (10);
- het verschaffen van een signaal ter indicatie van het vooraf bepaalde recht voor de aanbieder, als de chip (5) en de data authentiek zijn, de vooraf bepaalde
- 15 relatie is vastgesteld en de aanbieder gelijk is aan de houder.

7. Houder voorzien van een computerprogramma volgens conclusie 6.

8. Document voorzien van machine-leesbare houdergegevens en een chip (5), welke
20 chip (5) is voorzien van een verwerkingseenheid (14) en daarmee verbonden geheugen (16) en een invoer/uitvoer-eenheid (15), waarbij het geheugen (16) biometrische gegevens van een houder omvat, alsmede data die een vooraf bepaalde relatie tot de houdergegevens hebben, alsmede instructies om de verwerkingseenheid de volgende handelingen te laten verrichten:

- 25 • communiceren met een systeem volgens conclusie 1 om de authenticiteit van de chip (5) met behulp van een publieke sleutel coderingstechnologie te laten vaststellen;
- versturen van de biometrische gegevens van de houder en de data uit het geheugen (16) naar het systeem.

30

9. Document volgens conclusie 8, waarbij het document een reisdocument (6) is.

10. Document volgens conclusie 9, waarbij de chip (5) een integraal deel uitmaakt

van het reisdocument.

11. Document volgens een van de conclusies 8-10, waarbij de invoer/uitvoer-eenheid is ingericht voor contactloze communicatie.

5

12. Document volgens een van de conclusies 8-11, waarbij de chip (5) is ingericht als transponder-eenheid.

13. Document volgens een van de conclusies 8-12, waarbij de vooraf bepaalde relatie is gebaseerd op een HASH over de houdergegevens.

10

29003

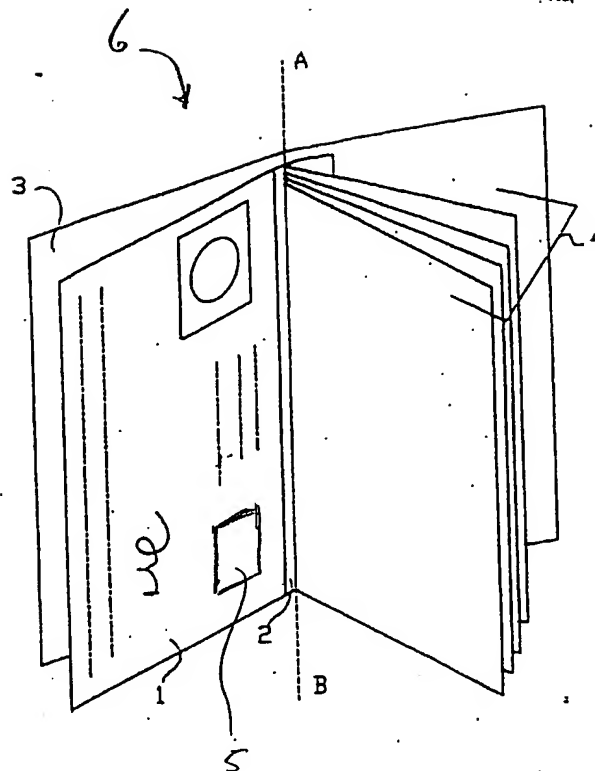


FIG. 1

1020903

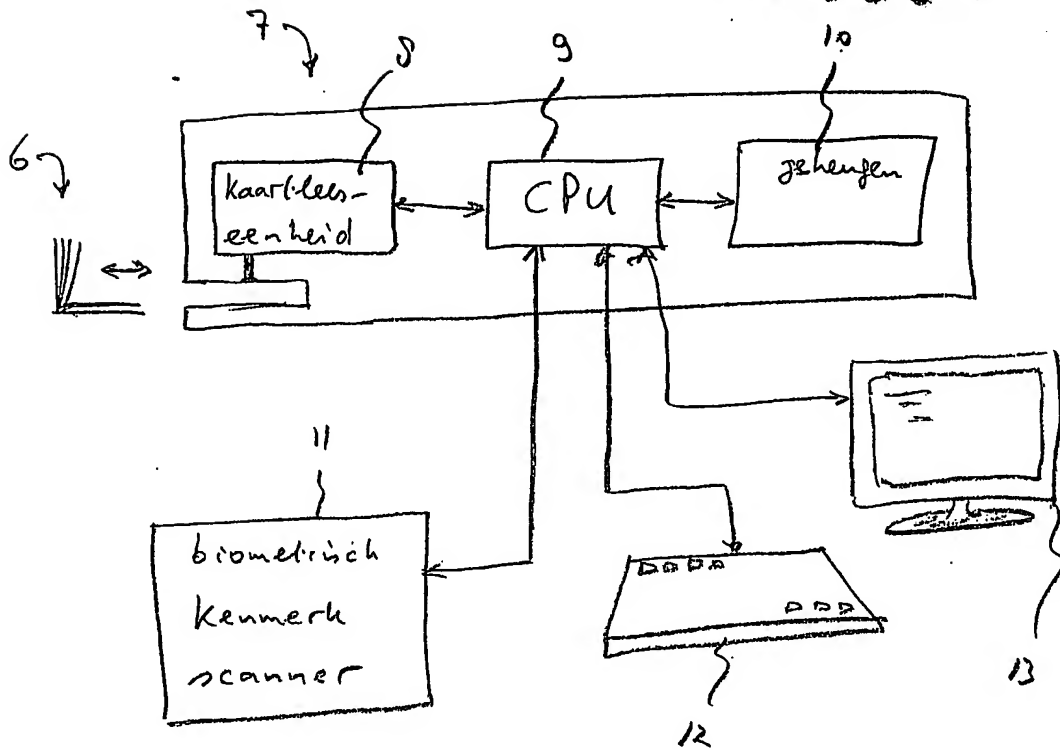


Fig. 2.

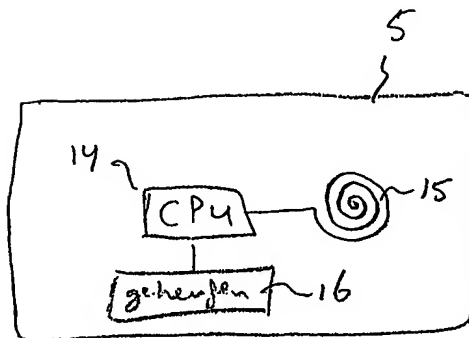


Fig. 3

1020903

EPO-DG 1
13 12 2004

(72)

Rec'd PCT/

16 DEC 2004

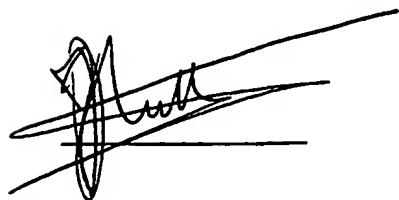
DECLARATION OF ENGLISH TRANSLATION OF PRIORITY DOCUMENT

I, HUTTER, Jacobus Johannes of The Hague

do hereby certify that I am conversant with the English and Dutch languages and am a competent translator thereof, and I further certify that to the best of my knowledge and belief the following is a true and correct translation made by me of the document in the Dutch language filed for a patent application in the Netherlands under No. 1020903 on 19 June 2002 in the name of Enschede/SDU B.V. at Haarlem, the Netherlands entitled:

" System and method for automatic verification of the holder of an authorisation document and automatic establishment of the authenticity and validity of the authorisation document ".

Signed this 23 November 2004



System and method for automatic verification of the holder of an authorisation document and automatic establishment of the authenticity and validity of the authorisation document

Prior Art

5

The system and the method to which the invention relates is applied in particular in checking passports at a border crossing. However, the invention can also be employed when obtaining access to a specific location or area or acquiring the right to access a system, such as a computer or a terminal, etc.

10

The method that is generally followed by an official at a border crossing is as follows:

- A. Checking the authenticity of a travel document and checking the authenticity of the information contained in the travel document, such as a passport, by looking at authenticity characteristics;
- 15 B. Verification whether the document that is being presented belongs to the person who is offering it (holder) by comparing the passport photograph and/or signature;
- C. Checking the validity of the document and permission to cross the border by typing in the passport number and/or the name of the holder for comparison with a database containing a stop register, that is to say a register containing a list of passport numbers and/or the names of holders who are not authorised to cross the border.

20

The use of biometry on a passport, supplementary to a passport photograph and signature, is also known and serves to support step B, verification of the document holder. Known biometric methods, which can also be used with the invention, comprise, for example, the use of one or more of the following personal characteristics (biometric template): eyes (iris), voice, handprints, fingerprints, face and handwritten signatures.

25

An obvious embodiment of a travel document with biometry is storage of the biometric template on the document. This can be, for example, in a 2D barcode, on a magnetic strip or in a chip.

30

In the case of automatic checking a disadvantage of this is that the biometric template is

linked to the personal details. This can be undesirable in connection with privacy. Another disadvantage is that a biometric template can be added to a travel document by an unauthorised person so that this unauthorised person is unjustifiably able to cross a border. It is also possible to present any arbitrary other (fake) document with a biometric template.

5 These forms of fraud then remain undetected in the case of automatic checking.

Brief summary of the invention

10 The aim of the invention is therefore to provide a system that does not have the abovementioned disadvantages.

To this end the invention first of all provides a system for reading a document provided with machine-readable holder details and establishing whether a person presenting the document has a predetermined right, which document at least contains a chip containing
15 biometric data on a holder as well as data with a predetermined relationship to the holder details, and wherein the system comprises:

- a reader for reading the chip and the machine-readable holder details;
- a memory containing details with regard to the predetermined right of the holder;
- a biometric feature scanner;
- 20 • a processing unit that is connected to the reader, the memory and the biometric feature scanner and is equipped to:
 - establish the authenticity of the chip and the data with the aid of a public key encryption technology;
 - receive the biometric data on the holder from the chip, from the reader;
 - 25 • receive the biometric data on the person presenting the document from the biometric feature scanner and to compare these with the biometric data on the holder to determine whether the person presenting the document is the holder;
 - receive the holder details via the reader, check the predetermined relationship between the holder details and the data and read the predetermined right of the
30 holder from the memory;
 - provide a signal to indicate the predetermined right for the person presenting the document if the chip and the data are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder.

In one embodiment the invention relates to a method for reading a document provided with machine-readable holder details and establishing whether a person presenting the document has a predetermined right, which document contains at least one chip containing biometric data on a holder as well as data having a predetermined relationship to the holder details, and wherein the system comprises a reader for reading the chip and the machine-readable holder details, a memory containing data on the predetermined right of the holder, a biometric feature scanner and a processing unit that is connected to the reader, the memory and the biometric feature scanner, wherein the method comprises the following operations:

- 10 • establishment of the authenticity of the chip and the data with the aid of a public key encryption technology;
- receipt of the biometric data on the holder from the chip;
- receipt of the biometric data on the person presenting the document and comparison with the biometric data on the holder to determine whether the person
- 15 presenting the document is the holder;
- receipt of the holder details, checking of the specific relationship between the holder details and the data and reading the predetermined right of the holder from the memory;
- provision of a signal to indicate the predetermined right for the person presenting
- 20 the document if the chip and the data are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder.

In a further embodiment the invention relates to a computer program that can be loaded by a system for reading a document provided with machine-readable holder details and establishing whether a person presenting the document has a predetermined right, which document contains at least one chip containing biometric data on a holder as well as data having a predetermined relationship to the holder details, and wherein the system comprises a reader for reading the chip and the machine-readable holder details, a memory

25 containing data on the predetermined right of the holder, a biometric feature scanner and a processing unit that is connected to the reader, the memory and the biometric feature scanner, wherein the computer program can provide the system with the following functionality:

30

- establishment of the authenticity of the chip and the data with the aid of a public key encryption technology;
 - receipt of the biometric data on the holder from the chip;
 - receipt of the biometric data on the person presenting the document and comparison with the biometric data on the holder to determine whether the person presenting the document is the holder;
 - receipt of the holder details, checking of the specific relationship between the holder details and the data and reading the predetermined right of the holder from the memory;
 - provision of a signal to indicate the predetermined right for the person presenting the document if the chip and the data are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder.
- 15 In yet a further embodiment the invention relates to a carrier provided with such a computer program.

- Finally, the invention also relates to a document provided with machine-readable holder details and a chip, which chip is provided with a processing unit and memory connected thereto and an input/output unit, wherein the memory contains biometric data on a holder, as well as data that have a predetermined relationship to the holder details, as well as instructions for making the processing unit carry out the following operations:
- communication with a system according to Claim 1 to enable the authenticity of the chip to be established with the aid of a public key encryption technology;
 - transmission of the biometric data on the holder and the data from the memory to the system;

By means of the invention it is possible automatically to establish that the document is authentic and that the person presenting the document actually is the holder thereof.

Description of the figures

The invention will be described in brief with reference to a few figures that are intended

solely for the purposes of illustration thereof and not to restrict the scope thereof, which is restricted only by the appended claims and their equivalents.

5 Figure 1 shows a document, in the form of a booklet, for example a passport, in which there is a chip containing biometric data;

Figure 2 shows a system by means of which the document as shown in Figure 1 can be read and evaluated;

10 Figure 3 shows, diagrammatically, a chip such as can be incorporated in the document according to Figure 1.

Description of embodiments

The invention will now be described with reference to the use of a passport as travel document. As stated above, the invention can, however, be applied more widely,
15 specifically wherever someone has to acquire a specific right in order to be able to do something.

Figure 1 shows the application of the invention in the case of a passport 6. With the exception of chip 5, the passport 6 as shown in Figure 1 has been described in detail in
20 European Patent Application EP-A 1 008 459. The passport as described in this publication, including all its embodiments, can be used with the present invention. The passport 6 contains a card 1 provided with text, a passport photograph and a signature. The card 1 can, for example, be made of synthetic laminate. The card 1 is fixed to a strip 2 that ensures that the card can be retained in the form of a booklet. Machine-readable holder
25 details are provided on the card 1.

The booklet contains further pages 4, suitable, for example, for recording visas for visits to countries. The booklet also has a cover 3. The reader is referred to European Patent Application EP-A 1 008 459 for further details and embodiments.

30

It is also pointed out that the invention can be used with other types of documents, but that use with a passport (or other travel document) is particularly advantageous because to date no watertight check for the authenticity of the document as well as verification of the

person presenting the document has been found for this purpose.

In accordance with the invention, the card 1 contains a chip 5. The chip is preferably integrated in the card 1 in such a way that this chip 5 cannot be removed without damaging the card 1.

Figure 3 shows one embodiment of such a chip 5. The chip 5 comprises a processing unit (CPU) 14, that is connected to a memory 16 as well as input/output unit 15.

10 The memory comprises, for example, ROM and a non-volatile memory, such as an EEPROM, but other types of memory can also be used. At least the following are stored in the memory: a private key (preferably in ROM, so that this cannot be changed), a biocertificate and (optionally) a certificate from an issuing authority. The biocertificate contains biometric feature data on the holder of the passport and data that have a
15 predetermined relationship with the machine-readable data.

The input/output unit 15 is preferably suitable for contact-free communication with the system that is shown in Figure 2. For this purpose the input/output unit 15 can preferably be made in the form of a circular antenna, as is shown in Figure 3. However, other
20 embodiments are possible. Contact surfaces, such as are known from current chip cards, are also possible.

It should be clear that Figure 3 shows only one embodiment. If desired, several processing units can have been provided, as well as several forms of memories and several
25 input/output units. Preferably, the chip 5 receives its power supply from the system that is shown in Figure 2 during communication therewith. For this purpose the chip 5 is therefore designed as a transponder unit. Such a transponder unit is known to those skilled in the art and does not have to be explained in detail here. Of course, a battery can be provided instead of this, although in the majority of cases this is highly impractical.

30

Figure 2 shows a system 7 for reading the chip 5 applied to the passport 6. For this purpose the system according to Figure 2 is equipped with a card reader 8, which is provided with a chip reader in order to communicate with the chip 5 on the card 1, and a reader for reading

the holder's details which, for example, are provided in a "machine readable zone" (MRZ) of the card 1.

5 The card reader 8 is connected to a processing unit (CPU) 9. The CPU 9 is connected to a memory 10.

10 The system 7 is also connected to a biometric feature scanner 11, as well as a keyboard 12 and a screen 13. The biometric feature scanner 11 is equipped to be able to scan a biometric feature of a person presenting the document 6. Such a scanner 11 can be, for example, an iris scanner or a device for reading a fingerprint from the person presenting the passport. Such biometric feature scanners 11 are known in the art and do not need to be described in detail here.

15 The structure of the system 7 from Figure 2 is arbitrary. If desired, all components can be accommodated in one cabinet. However, some components can also be housed in separate cabinets if desired. Apart from the keyboard 12, a mouse or other input/output means that are known to those skilled in the art can, for example, also be provided. The screen 13 can have any desired shape and can be of any desired type that is currently obtainable on the market (or will be so in the future).

20

It is indicated in Figure 2 that there is a memory 10. This memory can consist of RAM, ROM, EEPROM, a hard disk, etc., etc. The processing unit 9 can consist of a single unit but also of several units which may or may not be arranged in parallel or in a master/slave relationship. As a further alternative, various components can be installed remotely from one another. The memory 10 can, for example, be located a great distance away, if this is desirable.

The mode of operation of the system according to Figure 2 will now be explained with reference to a number of operations.

30

1. The passport 6 is submitted to the card reader 8 for reading the holder's details from the MRZ and reading data from the chip 5 on the passport 6;
2. The data read are transmitted to the CPU 9;

3. The CPU 9 transmits a random challenge code via the chip reader to the chip 5 to check the authenticity of chip 5 and requests the chip 5 digitally to sign or to encode this with the private key stored on the chip 5 belonging to the biocertificate stored on said chip;
- 5 4. The chip 5 then transmits the challenge code encoded or digitally signed with the private key back to the CPU 9. The encoded or digitally signed challenge code is the digital response. The chip 5 also transmits the biocertificate, as stored on the chip, signed with the private key of the issuing authority to the CPU 9. Optionally, the certificate from the authority that has issued the passport is also transmitted by
10 the chip 5 to the CPU 9. The sequence in which these data are transmitted by the chip 5 to the CPU 9 is arbitrary. It is also not absolutely essential to make use of one private key;
5. With the aid of the certificate from the issuing authority, the CPU 9 checks whether the biocertificate and the data that have been stored therein are authentic;
- 15 6. With the aid of the biocertificate, the CPU 9 checks whether the digital response is correct;
7. Data are stored in the biocertificate which can be used to check the relationship between the biocertificate and the holder's details. This can be, for example, by hashing the holder's details. The CPU 9 checks the relationship between the
20 biocertificate and the holder's details with the aid of the data in the biocertificate and the holder's details. The authenticity of the holder's details is also established by this means.
8. The biometric feature of the person presenting the passport is read by the biometric feature scanner 11 and this scanner transmits the data to the CPU 9. The CPU 9
25 converts these data into a biometric template (of course, the functionality for the conversion thereof can also be incorporated in the biometric feature scanner 11 by providing this with suitable intelligence for this purpose);
9. The CPU 9 checks, preferably via a one-way function (for example a hashing function), whether the passport number and/or the holder are listed in the stop
30 register stored in memory 10 and reports this to the official, for example via screen 13;
10. The CPU 9 checks whether the biometric template obtained from operation 8 corresponds to the biometric template from the biocertificate received from the

chip 5; the official will be informed of the result of this check, preferably via screen 13.

The invention eliminates the disadvantages that arise in the case of the "state of the art".

- 5 Specifically, it is possible by means of the abovementioned operations to check that both the passport and the holder's details are authentic and that the person presenting the passport is also actually the holder thereof. That is to say, secure automatic border control becomes possible by this means, which has not (yet) been the case to date.
- 10 By making use of the "biocertificate", the biometric template is not directly linked to the personal details. This is partly the case because the relationship between the biocertificate and the holder's details (for example the data in the MRZ) are linked to one another by a one-way function (hashing).
- 15 The authenticity of the information carrier (chip) is checked by signing the challenge code with the private key. The private key cannot be copied. By means of checking the biocertificate against the biometric template and the check on the authenticity of the chip 5, fraud is virtually precluded in the case of an automatic check. Moreover, chip 5 and the passport 6 are joined to one another such that they cannot be separated, as a result of which
- 20 manipulation of the chip 5 becomes impossible without causing discernible damage.

Claims

1. System for reading a document (6) provided with machine-readable holder details and establishing whether a person presenting the document (6) has a predetermined right, which document at least contains a chip (5) containing biometric data on a holder as well as data with a predetermined relationship to the holder details, and wherein the system comprises:
 - a reader (8) for reading the chip (5) and the machine-readable holder details;
 - a memory (10) containing details with regard to the predetermined right of the holder;
 - 10 • a biometric feature scanner (11);
 - a processing unit (9) that is connected to the reader (8), the memory (10) and the biometric feature scanner (11) and is equipped to:
 - establish the authenticity of the chip and the data with the aid of a public key encryption technology;
 - 15 • receive the biometric data on the holder from the chip, from the reader (8);
 - receive the biometric data on the person presenting the document from the biometric feature scanner (11) and to compare these with the biometric data on the holder to determine whether the person presenting the document is the holder;
 - receive the holder details via the reader (8), check the predetermined relationship between the holder details and the data and read the predetermined right of the holder from the memory (10);
 - 20 • provide a signal to indicate the predetermined right for the person presenting the document if the chip (5) and the data are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder.
2. System according to Claim 1, wherein the document is a travel document.
3. System according to Claim 1 or 2, wherein the processing unit (9) is equipped to compare the holder's details, using a one-way function, with holder's details stored in the memory (10).
- 30 4. System according to Claim 3, wherein the one-way function is a hashing function.

5. Method for reading a document (6) provided with machine-readable holder details and establishing whether a person presenting the document (6) has a predetermined right, which document contains at least one chip (5) containing biometric data on a holder as well
5 as data having a predetermined relationship to the holder details, and wherein the system comprises a reader (8) for reading the chip (5) and the machine-readable holder details, a memory (10) containing data on the predetermined right of the holder, a biometric feature scanner (11) and a processing unit (9) that is connected to the reader (8), the memory (10) and the biometric feature scanner (11), wherein the method comprises the following
10 operations:

- establishment of the authenticity of the chip and the data with the aid of a public key encryption technology;
- receipt of the biometric data on the holder from the chip;
- receipt of the biometric data on the person presenting the document and
15 comparison with the biometric data on the holder to determine whether the person presenting the document is the holder;
- receipt of the holder details, checking of the specific relationship between the holder details and the data and reading the predetermined right of the holder from the memory (10);
- 20 • provision of a signal to indicate the predetermined right for the person presenting the document if the chip (5) and the data are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder.

25 6. Computer program that can be loaded by a system for reading a document (6) provided with machine-readable holder details and establishing whether a person presenting the document (6) has a predetermined right, which document contains at least one chip (5) containing biometric data on a holder as well as data having a predetermined relationship to the holder details, and wherein the system comprises a reader (8) for reading the chip (5)
30 and the machine-readable holder details, a memory (10) containing data on the predetermined right of the holder, a biometric feature scanner (11) and a processing unit (9) that is connected to the reader (8), the memory (10) and the biometric feature scanner (11), wherein the computer program can provide the system with the following functionality:

- establishment of the authenticity of the chip (5) and the data with the aid of a public key encryption technology;
 - receipt of the biometric data on the holder from the chip (5);
 - receipt of the biometric data on the person presenting the document and comparison with the biometric data on the holder to determine whether the person presenting the document is the holder;
 - receipt of the holder details, checking of the specific relationship between the holder details and the data and reading the predetermined right of the holder from the memory (10);
 - provision of a signal to indicate the predetermined right for the person presenting the document if the chip (5) and the data are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder.
7. Carrier provided with a computer program according to Claim 6.
8. Document provided with machine-readable holder details and a chip (5), which chip (5) is provided with a processing unit (14) and memory (16) connected thereto and an input/output unit (15), wherein the memory (16) contains biometric data on a holder, as well as data that have a predetermined relationship to the holder details, as well as instructions for making the processing unit carry out the following operations:
- communication with a system according to Claim 1 to enable the authenticity of the chip (5) to be established with the aid of a public key encryption technology;
 - transmission of the biometric data on the holder and the data from the memory (16) to the system.
9. Document according to Claim 8, wherein the document is a travel document (6).
10. Document according to Claim 9, wherein the chip (5) is an integral part of the travel document.
11. Document according to one of Claims 8 - 10, wherein the input/output unit is equipped for contact-free communication.

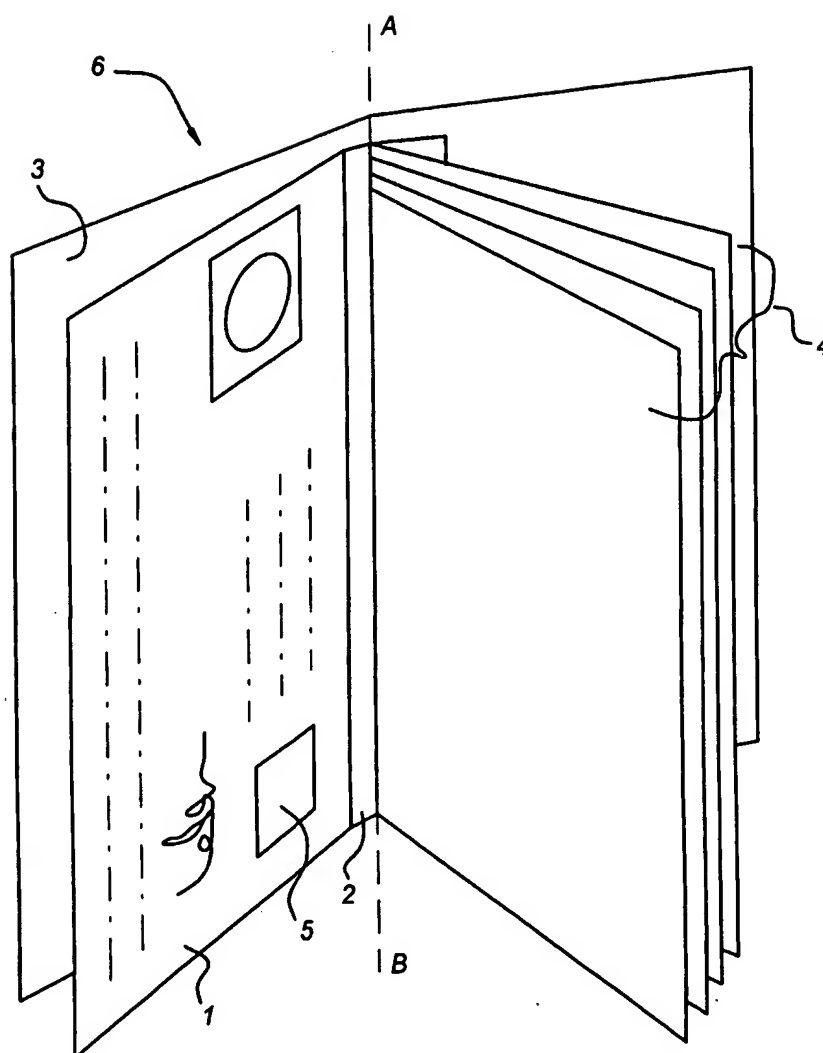
12. Document according to one of Claims 8 - 11, wherein the chip (5) is equipped as a transponder unit.
- 5 13. Document according to one of Claims 8 - 12, wherein the predetermined relationship is based on hashing the holder's details.

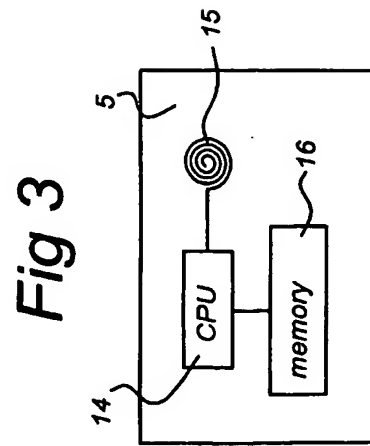
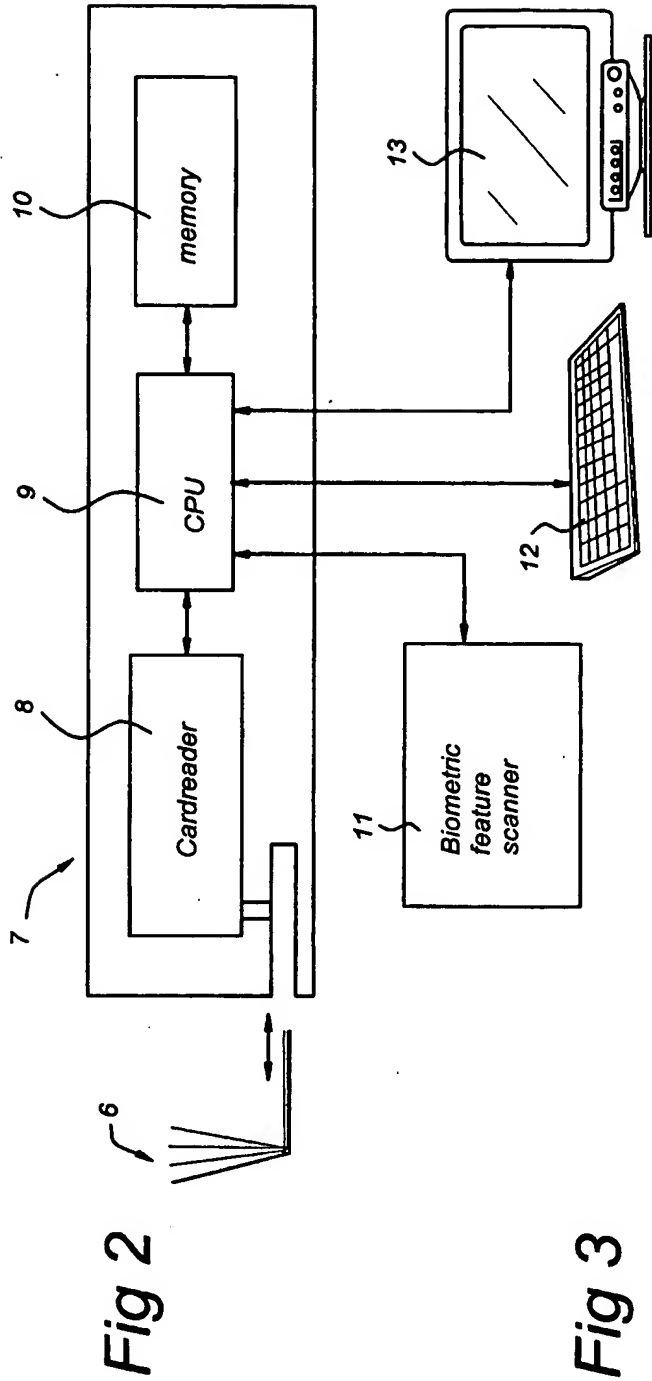
Abstract

System for reading a document provided with machine-readable holder details and establishing whether a person presenting the document has a predetermined right, which
5 document at least contains a chip containing biometric data on a holder as well as data with a predetermined relationship to the holder details, and wherein the system comprises:

- a reader for reading the chip and the machine-readable holder details;
 - a memory containing details with regard to the right of the holder;
 - a biometric feature scanner;
 - 10 • a processing unit connected to reader, memory and scanner and equipped to:
 - establish the authenticity of chip and data using public key encryption technology;
 - receive the biometric data on the holder from the chip;
 - receive the biometric data on the person presenting the document from the scanner and to compare these with the data on the holder to determine whether the person
15 presenting the document is the holder;
 - receive the holder details via the reader, check the relationship between the holder details and the data and read the right of the holder from the memory;
- provide a signal to indicate the right for the person presenting the document if the chip and the data are authentic, the relationship has been established and the person presenting the
20 document is the same as the holder.

Fig 1





**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☒ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☒ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.